METHOD FOR CONTROLLED AND AUDITED ACCESS TO PRIVILEGED ACCOUNTS ON COMPUTER SYSTEMS

Cross-Reference to Related Patent Application

This patent application is related to and claims the benefit of Provisional U.S. Patent Application No. 60/487,995, which application is hereby incorporated by reference in it entirety.

Field of the Invention

This invention relates to the field of limiting access to privileged accounts on computer systems, and, more specifically, to a method for providing controlled access to privileged accounts and sensitive data, wherein any access is reported to management and is fully auditable.

Background of the Invention

Computer security has become a critical issue in today's world. On one hand, enterprises are providing an ever-increasing number of services via computer systems for increasingly sophisticated, real-time transactions. At the same time, hacker break-ins, computer terrorism and employee (or former employee) sabotage is increasing. Thus, there is a tension between the need to keep computer system accessible for changes, upgrades and emergency fixes in order to keep business moving while preventing unauthorized access.

For example, sophisticated transactions involving stocks, bonds, derivatives, futures, *etc.*, and combinations thereof, are executed internationally. These transactions are carried out on one or more secure accounts on one or more computer systems. Such secure accounts include, but are not limited to, trading services, price-feed services and data-feed services. These secured accounts are referred to herein as "Privileged Accounts." It is clear that Privileged Accounts must be secure to prevent tampering, unauthorized acquisition of private data, *etc.* It is also clear that that Privileged Accounts must have some form of access to keep these accounts up-to-date and operative to prevent financial loss, incorrect or missing data, unconsummated time-sensitive transactions, *etc.*

Therefore, there is a need in the art for a secure system and method for accessing Privileged Accounts.

Summary of the Invention

This problem is solved and a technical advance is achieved in the art by a system and method that provides access to Privileged Accounts to users with Privileged Account access permission. The user must enter a reason for access. A message is sent to a Privileged Accounts manager when a user logs into a Privileged Account, which includes the user id, the account, the system and the reason. If the login is successful, all keystrokes are then logged. At the conclusion of the user session, the log file is closed and another message is sent to the Privileged Accounts manager. The log file may be sent to the manager at this time or saved for a batch transfer periodically.

According to an exemplary method of this invention, when a user attempts to log into an account, the account is verified against a list of Privileged Accounts that may be accessed. If the account is in the list, then the user is verified against a Privileged Account group. If the user is in the group, then the user is prompted for a reason for accessing the selected Privileged Account. A message is then sent to an account manager regarding the Privileged Account access, which may, advantageously, includes the user name or ID, the time and date, the Privileged Account being accessed and the reason.

If the login is successful, all key strokes are then recorded in a key log. Advantageously, the key log is duplicated. Further, if tampering is detected in the key log, the session is ended and the duplicate key log is sent to the account manager.

At the conclusion of the user session, the key log is closed and a second message sent to the account manager. This second message may include the key log file. Periodically, the key log files are collected and sent to a location for analysis and storage.

In this manner, security may be maintained on Privileged Accounts while permitting access to users that have permission. Further, management is informed of access to Privileged Accounts when they occur and can review all key strokes made by users.

Brief Description of the Drawings

A more complete understanding of this invention may be obtained from a consideration of this specification taken in conjunction with the drawings, in which:

FIG. 1 is a block diagram of a data network in which an exemplary embodiment of this invention may be implemented;

FIG. 2 is a flow chart of processing according to the exemplary embodiment of this invention;

FIG. 3 is a flow chart of further processing according to the exemplary embodiment of this invention;

FIG. 4 is a screen shot of an email message when a login failed during the processing of

FIG. 2;

FIG. 5 is a screen shot of a successful login during the processing of FIG. 2;

FIG.'s 6 and 7 are screen shots of email messages that a manger may receive for successful logins during the processing of FIG. 2;

FIG. 8 is a screen shot of an email message that a manger receives when the user tampers with the log file during the processing of FIG. 3;

FIG. 9 is a sample of a log file summary according to an aspect of this invention; and

FIG. 10 is a sample of a log file according to another aspect of this invention.

Detailed Description

FIG. 1 is a block diagram of an exemplary data network 100 used in effecting data flow and trading of instruments. While this invention is described in terms of a data network used for financial dealings, this invention may be used wherever security is required on a computer system. For example, a server for a web site may employ this invention. Also, a stand-alone system, such as a computer-controlled telephone exchange, may employ this invention. One skilled in the art will appreciate how to implement this invention in widely diverse applications after studying this specification.

Data network 100 comprises, in general, a plurality of users at user level 102 in communication with business layer 104 via data network 106. User level 102 comprises a plurality of user terminals, represented by workstation 110 and personal computer (PC) 112. Workstation 110, PC 112 or both can be used by traders or brokers in the investment community to, for example, obtain information and execute trades. Also illustrated in user layer 102 are workstations 114 and 116 connected to server 118. This server 118 and workstation 114, 116 community may be used, for example, by a brokerage house.

Business layer 104 comprises a plurality of servers, represented by servers 132, 134 and 138. By way of example, servers 132 and 134 comprise data servers connected to data storage components 138 and 140, respectively. Server 136 provides real-time data feeds from, for example, national data markets, international data markets or both. Terminal 138 and terminal 140 comprise command and maintenance terminals, as known in the art. These terminals permit authorized users to access servers 132 and 136, respectively, in order to perform regular maintenance and to fix real-time problems. Server 134, in this exemplary embodiment, provides for remote access from, for example, terminal 148 for maintenance.

Data network 106 comprises, in this exemplary embodiment, the Internet. While data network 106 is described in terms of the Internet, any public or private data network may be used. PC 150 and PC 152 are illustrated herein as being connected to data network 106. PC 150 and PC 152 represent remote access terminals for remote administration of server 132, server 134 and server 136. Further, PC 150 and PC 152 represent regional or national management of business layer 104.

In the context of data network 100, business layer 104, and, more specifically, server 132, server 134 and server 136, are the primary users of an exemplary embodiment according to this invention. Server 132, server 134 and server 136 all contain data and transaction information that must remain confidential, proprietary or maintain a constant flow. Each service provided by these servers comprises an account on the server. In terms of this invention, each service provided by server 132, server 134 and server 136 comprises a Privileged Account, which is protected by an exemplary embodiment of this invention.

In the exemplary embodiment of this invention, UNIX is the operating system used in server 132, server 134 and server 136. While this invention is described in terms of the UNIX operating system (and its variants), one skilled in the art will appreciate how to apply the principals of this invention to other operating systems after studying this specification.

In accordance with the exemplary embodiment of this invention, a user at terminal 138 wants to apply a change request ("CR") in order to, for example, fix a known bug. The user logs in as usual and executes the "switchuser" (su) command to a selected Privileged Account in order to access to that Privileged Account. In the prior art, all the user would have to know is the password for "su," and the user can do anything to the account.

According to this invention, an "suwrapper" is placed around the usual UNIX su command. The usual UNIX su command is disabled to access certain accounts. Turning now to FIG.'s 2 and 3, a flow chart of processing in accordance with this embodiment of this invention is shown. In input box 202, the user invokes the su command with an account name as an argument. The method according to this invention first retrieves a list of Privileged Accounts that can be accessed by this method in box 204. If, in decision diamond 206, the account is not in the list, then the user is permitted to su into it under the usual UNIX su command in box 210. Processing continues along arrow 212.

If the selected account is in the Privileged Accounts list in decision diamond 214, then the user id is verified against a group list. If the user is not in the privileged group, the user is denied access in box 216 and a system manager is notified in box 218. FIG. 4 is a screen shot of such email to a manager. Information sent to the manager should be satisfactory to trace who tried to log into a Privileged Account, so that person may be dealt with in an appropriate manner.

If the user is in the privileged group as determined at decision diamond 214, then a screen as illustrated in FIG. 5 is displayed to the user. First, at 502 the user is prompted for a reason for the access. The user responds with a reason at 504. Logging in proceeds and the user is asked for the user's password at 506. Using the user's password at 506 prevents the user from knowing other accounts passwords. As is known in the art, the password is then verified and the system displays a warning screen, such as the warning screen at 508. The user is now logged in.

Returning to FIG. 2, an email message is sent to the manager in box 226. Sample email messages are shown in FIG.'s 6 and 7. Both email messages include the date, the Privileged Account, the system and the reason. Additionally, the key log file is noted in the email so that the manager may access the file if necessary. Processing proceeds to FIG. 3 in connector 228.

Turning now to FIG. 3, processing continues from FIG. 2 at connector 300. At this point, the user is successfully logged in. The next four operations occur approximately simultaneously, as is known in the art, and are thus presented here in an order that facilitates flowcharting.

Processing continues in the context of the flowchart of FIG. 3 in box 302, where keystrokes are logged to a file. In box 304, keystrokes are logged to a duplicate file. In this manner, if the user attempts to tamper with the log file, the duplicate file is still available for managers to review and take action on.

In decision diamond 306, a determination is made whether the user logged out. If not, then processing moves to decision diamond 308, where a determination is made whether the user tampered with the log file. If the user did not tamper with the log file, then processing loops back to box 302.

If, in decision diamond 306, the user did tamper with the log file, then that fact is recorded in the duplicate log file in box 310. The login is terminated in box 312.

Processing from both the "YES" branch of decision diamond 306 (the user logged out) and box 312 moves to box 314 where the log file is stored. In this exemplary embodiment, the log file is made read-only for security and compressed ("zipped") to preserve space. In box 316, email is again sent to the manager. FIG. 8 illustrates the email received when the user tampered with the log file. The users name is included along with the other data, according to this exemplary embodiment.

At some time 320 (immediately, hourly, daily, *etc.*), the log file is sent to the manager in box 322. Processing concludes in oval 324.

According to this embodiment of this invention, log files are displayed in two ways. Turning to FIG. 9, a first log file format is shown. This log file format presents a summary of all of the logins on all of the systems that this manager monitors. Generally, this summary presents the name of the system ("HOST"), the time of the login ("LOGIN"), the time of the logout ("LOGOUT"), the user ("WHO"), the reason ("REASON") and any comments. In this manner, the manager can tell at a glance what has happened in the past time period.

Turning now to FIG. 10, a detailed log file is shown. All of the operations performed by the users are shown specifically. In this manner, the manager may trace any tampering, wrong entries, *etc.*, and is able to take appropriate action immediately.

Advantageously, additional protections may be afforded to suwrapper configuration files and audit logs. In accordance with one exemplary embodiment of this invention, the suwrapper script is owned by root and write protected. Furthermore, suwrapper may be programmed such that, if someone attempts to run the script in the debugging mode ("-x" switch), the script immediately exits.

In accordance with other aspects of this invention, configuration files are owned by root and write protected. Log files, while owned by the user, are zipped and write protected when suwrapper exits. Further, all files that support suwrapper may advantageously be protected by the optional layered security tool called "eTrustAC" (previously called SEOS and referenced above).

It is to be understood that the above-described embodiment is merely illustrative of the present invention and that many variations of the above-described embodiment can be devised by one skilled in the art without departing from the scope of the invention. It is therefore intended that such variations be included within the scope of the following claims and their equivalents.